David Hilton Wise, Esq.
Nevada Bar No. 11014
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro

Howard T. Longman *(pro hac vice forthcoming)*
LONGMAN LAW, P.C.
354 Eisenhower Parkway, Suite 1800
Livingston, New Jersey 07039
Tel: (973) 994-2315
Fax: (973) 994-2319
Email: hlongman@longman.law

Gary S. Graifman *(pro hac vice forthcoming)*
Melissa R. Emert *(pro hac vice forthcoming)*
KANTROWITZ GOLDHAMER & GRAIFMAN, P.C.
16 Squadron Blvd Suite 106,
New City, N.Y. 10956
Tel: (845) 356-2570
ggraifman@kgglaw.om
memert@kgglaw.com

Attorneys for Plaintiffs and the Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

JEFFREY RUDERMAN and LAURA RUDERMAN, for themselves and S.R., a minor, and all others similarly situated, *Plaintiffs*, v. NORTHWELL HEALTH, INC. and PERRY JOHNSON & ASSOCIATES, INC. *Defendants*.	Case No. 2:23-cv-02014 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Jeffrey Ruderman and Laura Ruderman, for themselves and their daughter S.R., a minor (collectively "Plaintiffs"), and on behalf of all others similarly situated, bring this Class Action Complaint against Northwell Health, Inc. ("Northwell") and Perry Johnson & Associates, Inc. ("PJ&A") (collectively "Defendants"), and allege, upon personal knowledge as to their own actions and the investigation of counsel, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises from a cyberattack and data breach (the "Data Breach") resulting in the acquisition of sensitive and private information in the possession and custody and/or control of Defendants.

2. Plaintiffs Jeffrey and Laura Ruderman each received a letter from PJ&A dated November 3, 2023, informing them that their private information had been compromised in the Data Breach. They received a third letter pertaining to S.R., stating that her private information was also compromised.

3. The three letters (the "Notice Letters") state that PJ&A provides transcription and dictation services to Northwell and receives personal health information regarding Northwell patients in the course of providing this information. Specifically, according to the letters, PJ&A received information including Plaintiffs' names, dates of birth, address, medical record numbers, hospital account numbers, treatment facilities, healthcare providers, admission diagnoses, and dates and times of service. According to the letter sent to Plaintiff Jeffrey Ruderman, PJ&A also was in possession of files containing transcripts of operative reports, consult reports, history and physical exams, discharge summaries, and progress notes that may have included reasons for visits, diagnoses, laboratory and diagnostic testing results, family medical history, surgical history, social history, medications, allergies, and/or other observational information. All of this information was illegally accessed and downloaded during the Data Breach.

4. The Notice Letters further state that the Data Breach occurred between March 27, 2023 and May 2, 2023, and that information specifically pertaining to Northwell patients was illicitly accessed

and downloaded between April 7, 2023 and April 19, 2023. PJ&A initially discovered that Northwell data was affected on May 22, 2023, but did not inform Northwell until July 21, 2023. By September 28, 2023, PJ&A states it had confirmed the scope of the Northwell patient information that was compromised.

5. The Notice Letters further state that Northwell arranged for Plaintiffs to receive one free year of identity protection from Experian Identity Works ("Experian").

6. The Data Breach exposed Defendants' negligence and breach of legal and equitable duties to protect and safeguard the sensitive Personal Identifying Information ("PII") and Personal Health Information ("PHI") (collectively, "Private Information") from unauthorized access and exfiltration. Defendants failed to protect, encrypt or even redact this private information for services Plaintiffs provided to Lenox Hill Hospital, a Northwell Health affiliate hospital, in connection with medical services provided from 2012 through 2023, leaving Plaintiffs and other patients of Defendants exposed to drastically heightened risk of identity theft. The present and continuing risk to victims of the Data Breach will last throughout their respective lifetimes.

7. The Notice Letters, which were not sent out until more than six (6) months after Plaintiffs' Private Information was stolen, downplayed the nature of the breach and the threat that it posed to victims whose Private Information was illicitly accessed and stolen. Defendants failed to inform Plaintiffs why Defendants took so much time to begin notifying victims that hackers had gained access to their Private Information.

8. Defendants' failure to timely report the Data Breach made its customers more vulnerable to identity theft, as those customers received no warnings to attempt to prevent unauthorized use of their stolen Private Information.

9. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance to mitigate the damage caused by infiltrators misusing their Private Information.

10. By failing to adequately protect Plaintiffs' and the Class's Private Information, failing to adequately notify them about the breach, and by obscuring the nature of the breach, Defendants violated state and federal law and further harmed millions of victims.

11. Plaintiffs and members of the proposed Class are victims of Defendants' negligence and inadequate cybersecurity measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendants with their Private Information, but Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent or mitigate the impact of the Data Breach.

12. Following the Data Breach, the victims' Private Information is permanently exposed and unsecured.

13. Accordingly, Plaintiffs, on their behalf and on behalf of a class and subclass of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because there are 100 or more class members, Plaintiffs and at least one class member are citizens of a state that is diverse from at least one Defendants' citizenship, and the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

15. This Court has personal jurisdiction over Defendants because the tortious harm inflicted on Plaintiffs and the Class emanated from PJ&A's headquarters in Henderson, Nevada. Defendant PJ&A is registered to do business in the State of Nevada, and has purposefully directed their actions towards Nevada, and/or have the requisite contacts with Nevada necessary to permit the Court to exercise jurisdiction.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant PJ&A

maintains its principal headquarters and offices within this District, has maintained and stored the exfiltrated data within this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

17. Plaintiff Jeffrey Ruderman is a citizen of New Jersey and is a victim of the Data Breach. He received care at Lenox Hill Hospital, a Northwell institution, and provided his Private Information to Northwell in the course of receiving that care. Based on representations made by Northwell, he believed that Northwell would adequately secure and protect his Private Information.

18. Plaintiff Laura Ruderman is a citizen of New Jersey and is a victim of the Data Breach. She received care at Lenox Hill Hospital and provided her Private Information to Northwell in the course of receiving that care. Based on representations made by Northwell, she believed that Northwell would adequately secure and protect her Private Information.

19. S.R., a minor, is a citizen of New Jersey and is a victim of the Data Breach. S.R. was born and received postnatal care at Lenox Hill Hospital and provided her Private Information to Northwell in the course of receiving that care. Based on representations made by Northwell, her parents and legal guardians, Plaintiffs Jeffrey and Laura Ruderman, believed that Northwell would adequately secure and protect her Private Information.

20. Defendant Northwell Health, Inc. is a New York not-for-profit corporation headquartered at 2000 Marcus Avenue, New Hyde Park, NY 11042. Northwell is the largest healthcare provider in New York State, operating more than twenty hospitals and almost nine hundred outpatient facilities. As of August of 2023, Northwell operates a multispecialty physician practice in Edgewater, New Jersey.

21. Defendant Perry Johnson & Associates is a Nevada corporation headquartered at 1489 W Warm Springs Rd., Henderson, NV 89014. PJ&A provides transcription services to clients in the medical and legal industries and government agencies.

STATEMENT OF FACTS

22. In the regular course of business, Northwell collects and retains the sensitive Private Information of its current and former patients. This information is collected as a necessary condition of providing care to patients.

23. Northwell states in its "Patient privacy overview" that "[o]ur patients are our number one priority and we believe that patient privacy is an integral part of the health care we provide to you." It further states that "[t]o ensure the development of a lasting bond of trust with our patients, we have many safeguards to protect the privacy and security of your personal information."

24. Northwell's privacy overview provides identity theft statistics, clarifying that it was well aware of the importance of safeguarding sensitive Private Information. Northwell had a duty to its patients to employ vendors with reasonable security measures in place to safeguard patients' sensitive Private Information

25. Northwell's Notice of Privacy Practices states that "[w]e may share your protected health information with a business associate that we hire to help us, such as a billing or computer company or transcription service. Business associates will have assured us in writing that they will safeguard your protected health information as required by law."

26. According to this statement, PJ&A assured Northwell in writing that it would safeguard the highly sensitive Private Information that it received in the course of providing its transcription services. Northwell's patients were the beneficiaries of that written assurance.

27. According to the U.S. Department of Health and Human Services ("HHS"), the Health Information Technology for Economic and Clinical Health ("HITECH") Act extended liability for violation of certain HIPAA rules to business associates who would not otherwise be covered under HIPAA, such as PJ&A. *See* 42 U.S.C. § 17931 (extending 45 C.F.R. § 164.308, 164.310, 164.312, and 164.316 to cover business associates), 45 C.F.R. § 164.410, 45 C.F.R. § 164.412, and 45 C.F.R. § 164.502(a)(3-4), (b), and

(e). PJ&A acknowledged that it was bound under HIPAA requirements as modified by the HITECH Act in its "Cyber Incident Notice" posted on its website, stating that "[t]his notice is being provided . . . in accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act."

28. Among these rules is 45 C.F.R. § 164.410, which requires business associates to provide notification of data breach "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." Despite this rule, PJ&A's notice letters to Northwell patients were dated November 3, 2023, more than five (5) months after discovery that Northwell patients were impacted by the breach. The tardiness of the notification violates the HIPAA rule as well as all applicable state laws regarding data breach notification. Defendants did not provide any acknowledgement of or explanation for the delay in notifying the data breach victims.

29. Almost 3.9 million Northwell patients were affected by the Data Breach. In total, nearly nine million individuals were affected by the breach. The breach has been described as "one of the largest healthcare data breaches ever discovered."

30. Defendants have not provided any indication that the illegally accessed and downloaded Private Information was encrypted in any way or otherwise protected by security measures that meet the standards of the industry or guidance of HIPAA, Children's Online Privacy Protection Act ("COPPA"), and the Federal Trade Commission Act ("FTC"), or their own contractual representations.

31. Defendants have not provided any information about the cause of the Data Breach, the vulnerabilities exploited, or the cybercriminals who perpetrated the attack and now hold Plaintiffs' and Class Members' Private Information.

32. Plaintiffs' and Class Members' Private Information is likely to be misused by the cybercriminals, or else sold to other criminals who will misuse the information for personal profit at the great expense of Plaintiffs and Class Members. Plaintiffs and Class Members must now take expensive

steps to safeguard their identities indefinitely, as their Private Information will be exposed forever.

33. Defendants recognized the actual imminent harm and injury that flowed from the Data Breach, as acknowledged in the Notice Letters. However, Defendant offered merely one year of complimentary identity theft protection services to victims, which does not adequately begin to address the lifelong harm that victims will face following the Data Breach.

34. Even with free identity theft protection services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' Private Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

35. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and related industries preceding the date of the breach.

36. In light of recent high profile data breaches at other healthcare providers and similar companies that handle sensitive private information, Defendants knew or should have known that their electronic records and patients' Private Information would be targeted by cybercriminals.

37. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

38. Indeed, cyberattacks against industries such as healthcare and insurance have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."

39. Cyberattacks on healthcare providers and similar companies have become so notorious that

the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

40. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

41. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendants.

42. As a result of Defendants' failure to protect Plaintiffs and the proposed Class Members' Private Information, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

43. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

44. The value of Plaintiffs' and the Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen Private Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

45. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

46. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

47. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

48. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify such information as Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz

package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

49. Defendants disclosed the Private Information of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the Private Information of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

50. Defendants' failure to promptly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants Failed to Adhere to FTC Guidelines

51. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of Private Information.

52. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of Private Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

53. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

54. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Comply with HIPAA and COPPA

57. As described above, both defendants are at least partially covered by the regulations of HIPAA. Both defendants are also covered by COPPA, which pertains to any operator of online services "that has actual knowledge that it is collecting or maintaining personal information from a child." 15 U.S.C. § 6502(a)(1).

58. Pursuant to HIPAA, Defendants had a duty to securely store and maintain patient

information and provide timely notification when that information was breached.

59. Pursuant to the COPPA, 15 U.S.C. § § 65-1=6505, Defendants had a duty to: (i) get parental consent before collecting personal information from children under 13; (ii) provide parents with the right to review and delete their children's information; and (iii) could only retain children's personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected, and thereafter had a duty to delete any and all child's personal information using reasonable measures to ensure it's been securely destroyed, even absent a parent's request for the deletion of a child's personal information. S.R. and minor Class Members are among the individuals whom COPPA is intended to protect. *See Under COPPA, data deletion isn't just a good idea. It's the law*. FTC, (May 31, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/05/under-coppa-data-deletion-isnt-just-good-idea-its-law [https://perma.cc/JWT2-KK3L].

Defendants Failed to Comply with Industry Standards

60. As noted above, experts studying cybersecurity routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

61. Several best practices have been identified that at a minimum should be implemented by businesses in possession of Private Information, like Defendants, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. On information and belief, Defendants failed to follow these industry best practices.

62. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and

routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. On information and belief, Defendants failed to follow these cybersecurity best practices.

63. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

64. The foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

65. Plaintiffs bring this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of a Nationwide Class and a New Jersey Subclass defined as:

The Nationwide Class is defined as:

> All individuals who received a Notice Letter from Defendants notifying them that their Private Information was compromised in the Data Breach.

The New Jersey Subclass is defined as:

> All individuals residing in New Jersey who received a Notice Letter from Defendants, notifying them that their Private Information was compromised in the Data Breach.

66. Excluded from the Class and Subclass are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

67. Plaintiffs reserve the right to amend the class and subclass definitions.

68. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under F.R.C.P. Rule 23.

a. **Numerosity**. The members of the Class and Subclass are so numerous that joinder would be impracticable. The number of class members is known to exceed 3.8 million.

b. **Ascertainability**. Members of the Class and Subclass are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiffs' claims are typical of class and subclass claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's and Subclass's interests. Their interests do not conflict with the Class's and Subclass's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's and Subclass's claims raise predominantly common fact and legal questions that a class-wide proceeding can answer for the Class and Subclass. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Private Information;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing

Private Information;

iv. Whether Defendants breached contract promises to safeguard Plaintiffs' and the Class's Private Information;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class and Subclass are entitled to damages, treble damages, or injunctive relief.

69. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(Against All Defendants)

70. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

71. Plaintiffs and members of the Class entrusted their Private Information to Defendants. Defendants owed to Plaintiffs and the Class a duty to exercise reasonable care in handling and using the Private Information in their care and custody, including following FTC and HIPAA guidelines and implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access. This includes following the FTC guidance on deleting

Private Information that is no longer needed.

72. Defendants owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their Private Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Private Information —just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's Private Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

73. Defendants owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

74. Defendants owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiffs' and the Class's Private Information.

75. The risk that unauthorized persons would attempt to gain access to Private Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Private Information, much of it over long periods of time without any valid business or medical purpose, it was inevitable that unauthorized individuals would attempt to access Defendants' data containing the Private Information, whether by malware or otherwise.

76. Private Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and the Class and the importance of exercising reasonable care in handling it and timely deleting any Private Information that was no longer needed.

77. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the Private Information of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

78. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(Against All Defendants)

79. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

80. Pursuant to the HIPAA privacy and security rules and the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Private Information.

81. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers' Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs' and the members of the Class's Private Information.

82. Defendants breached their duties to Plaintiff and Class Members under HIPAA and the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

83. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their consumers, which is recognized by laws and regulations as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach but failed to do so.

84. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

85. Defendants violated their duty under HIPAA and the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's Private Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to

individuals in the event of a breach, which ultimately came to pass.

86. The harm that has occurred is the type of harm that HIPAA and the FTC Act are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

87. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiffs and members of the Class would not have been injured.

88. The injury and harm suffered by Plaintiffs and members of the Class and Subclass were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to fulfill their duties and that such a breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

89. Had Plaintiffs and the Class known that Defendant did not adequately protect their Private Information, Plaintiffs and members of the Class would not have entrusted Defendant with their Private Information.

90. Defendants' various violations and their failure to comply with applicable laws and regulations constitute negligence *per se*.

91. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Private Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Private Information, entitling them to damages in an amount to be proven at trial.

92. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs

and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Private Information in their continued possession.

COUNT III
Breach of Fiduciary Duty
(Against Defendant Northwell Health, Inc.)

93. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

94. Plaintiffs and Class Members provided their Private Information to Northwell in confidence, believing that Northwell would adequately secure and protect that information. Plaintiffs and Class Members would not have entrusted Northwell with their Private Information had they believed that Northwell would not or could not adequately protect it. Northwell's acceptance and storage of that Private Information created a fiduciary relationship between Northwell and Plaintiffs and Class Members. In light of this relationship, Northwell must act primarily for the benefit of its patients, including by securing and safeguarding the sensitive Private Information in their care.

95. Once Plaintiffs and Class Members entrusted Northwell with their Private Information, they became entirely reliant on Northwell to adequately protect that information. Plaintiffs and Class Members had no means of verifying or determining the nature and extent of Northwell's compliance with its privacy policy or the security of their vendors, and Northwell was in an exclusive position to take steps to prevent the Data Breach.

96. Northwell has a fiduciary duty to act for the benefit of its patients in all matters within the scope of their relationship. It breached that duty by contracting with a vendor that could not or would not adequately protect and safeguard the sensitive Private Information of Northwell's patients, failing to comply with the data security guidelines set forth by HIPAA, COPPA, and the FTC, and otherwise failing

to protect the Private Information it collected. Northwell further breached that duty by failing to provide timely and adequate notice to its patients that their sensitive Private Information had been illegally accessed and downloaded.

97. As a direct and proximate result of Northwell's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury and damages of an amount to be determined at trial.

COUNT IV
Breach of Implied Contract
(Against Defendant Northwell Health, Inc.)

98. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

99. Plaintiffs and Class Members provided their Private Information to Northwell in order to receive medical care. In doing so, they entered into implied contracts under which Northwell agreed to secure and protect that information and provide timely and sufficient notice of any unauthorized disclosures.

100. Northwell represented to Plaintiffs and Class Members that they would secure and protect patients' Private Information. Plaintiffs and Class Members would not have entrusted Northwell with their Private Information had they believed that Northwell would not or could not adequately protect it.

101. Without the existence of the implied contracts, Plaintiffs and Class Members would not have entrusted Northwell with their Private Information.

102. Plaintiffs and Class Members fully performed their obligations under the implied contracts.

103. Defendants breached the implied contracts by failing to adequately protect Plaintiffs' and Class Members' Private Information, resulting in the Data Breach and the resulting injuries to Plaintiffs and Class Members. Defendants further breached the implied contracts by not providing timely and adequate notice of the Data Breach, thereby preventing Plaintiffs and Class Members from promptly taking steps to mitigate their injuries.

104. As and direct and proximate result of Northwell's breaches of the implied contracts, Plaintiffs and Class Members were injured and sustained actual losses and damages of an amount to be determined at trial.

COUNT V
Third-Party Beneficiary Claim for Breach of Contract
(Against Defendant Perry Johnson & Associates, Inc.)

105. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

106. As explained in Northwell's privacy policy, Northwell received written assurance from all business associates who received patients' Private Information that they would safeguard that information as required by law. On information and belief, Northwell received such written assurance from PJ&A as part of their contract for transcription and dictation services. This clause was intended to benefit Plaintiffs and Class Members, whose Private Information was being entrusted to PJ&A's care.

107. PJ&A breached their contract with Northwell, and in particular the clause that existed for the benefit of Plaintiffs and Class Members, by failing to adequately protect patients' Private Information, which directly resulted in the Data Breach. As a result of the breach, Plaintiffs and Class Members were injured.

108. As the intended third-party beneficiaries of the data security provisions in the contract between Northwell and PJ&A, Plaintiffs and Class Members are entitled to enforce its terms. The benefits that Plaintiffs and Class Members receive are not incidental to the purpose of the agreement. Indeed, the data security provisions in the contract would not exist but for the benefit of Plaintiffs and Class Members.

109. Northwell did not receive the full benefit of its bargain because PJ&A failed to protect Plaintiffs' and Class Members' Private Information as it had promised to do.

110. As a direct and proximate result of PJ&A's breach of its contract with Northwell, Plaintiffs and Class Members have suffered and will suffer injuries and damages of an amount to be determined at

trial.

COUNT VI
Unjust Enrichment
(Against All Defendants)

111. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

112. Plaintiffs and members of the Class conferred a benefit upon Defendants in providing Private Information to Defendants.

113. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and the Class. Defendants also benefited from the receipt of Plaintiffs' and the Class's Private Information, as this was used to facilitate the services and goods it provided to its patients, including Plaintiffs and the Class.

114. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs and the Class's Private Information because Defendants failed to adequately protect their Private Information. Plaintiffs and the proposed Class would not have provided their Private Information to Defendants had they known Defendants would not adequately protect their Private Information.

115. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct.

COUNT VII
Violation Of The New York Deceptive Trade Practices Act ("GBL")
(New York Gen. Bus. Law § 349)
(Against Defendant Northwell Health, Inc.)

116. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

117. Northwell engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct

of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiffs and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiffs and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Private Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' Private Information;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiffs and Class Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

118. Northwell knew or should have known that its data security practices were inadequate to safeguard Plaintiffs and Class Members' Private Information entrusted to them, and that the risk of a data breach or theft was highly likely.

119. Northwell should have disclosed this information because Northwell was in a superior position to know the true facts related to the defective data security.

120. Northwell's failure constitutes false and misleading representations, which have the

capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding Northwell's aggregation and handling of Private Information, including but not limited to failing to encrypt, redact, and/or otherwise protect that information.

121. The representations upon which consumers (including Plaintiffs and Class Members) relied were material representations (e.g., as to Northwell's adequate protection of Private Information), and consumers (including Plaintiffs and Class Members) relied on those representations to their detriment.

122. Northwell's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances, including acts and practices that would violate Section 5(a)(1) of the FTC Act, 15 U.S. C. § 45(a)(1),15 U.S.C. § 6801, et seq., HIPPA, 42 U.S.C. § 1301d, and COPPA, 15 U.S.C. § § 6501-05 .

123. As a direct and proximate result of Northwell's conduct, Plaintiffs and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

124. Northwell's acts, practices, and omissions were done in the course of Northwell's business of providing healthcare services to consumers in the State of New York.

125. As a direct and proximate result of Northwell's unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing and continuing to cause damages to Plaintiffs and the Class.

126. As a direct and proximate result of Northwell's multiple, separate violations of GBL §349, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and Class Members include: (a) the invasion of privacy;

(b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including the cost of credit and identity theft monitoring as well as loss of productivity; (d) monetary costs

associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Northwell promised when Plaintiffs and the proposed class entrusted Northwell with their Private Information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' Private Information, which remains in the Northwell's possession with inadequate measures to protect Plaintiffs' and Class Members' Private Information.

127. As a result, Plaintiffs and Class Members have been damaged in an amount to be proven at trial.

128. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members and the public fromNorthwell's unfair, deceptive, and unlawful practices. Northwell's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

129. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, in junctive relief, and/or attorney's fees and costs.

130. On behalf of himself and other members of the Class, Plaintiffs seek to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

131. As a direct result of Northwell's violation of GBL § 349, Plaintiffs and Class Members are also entitled to damages as well as injunctive relief, including, but not limited to, ordering Northwell to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual

audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VIII
Violation Of New York Gen. Bus. Law § 899-aa
(Against Defendant Northwell Health, Inc.)

132. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

133. According to the Notice Letters, Northwell learned of the Data Breach on July 21, 2023, but Plaintiffs and Class Members were not sent notice until November 3, 2023.

134. Pursuant to Gen. Bus. Law § 899-aa(2), Northwell was required to provide disclosure to the victims of a data breach within "the most expedient time possible and without unreasonable delay. . . ."

135. Northwell violated the statute by waiting more than three (3) months to notify Plaintiffs and Class Members of the data breach.

136. As a result of Northwell's unwarranted and unreasonable delay in notifying the data breach victims, the victims were unaware that their Private Information had been illegally accessed and stolen and that they were at drastically increased risk of being subject to identity theft. Had they known sooner, they could have taken immediate steps to protect their identities and prevent further injury.

137. As a result of Northwell's violation of the statute, Plaintiffs and Class Members were injured and demand all remedies warranted by law.

COUNT IX
Violation Of The New Jersey Consumer Fraud Act
(N.J. Stat. Ann. § 56:8-1 *et seq.*)
(On Behalf of the New Jersey Subclass against Defendant Northwell Health, Inc.)

138. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

139. The deceptive and misleading statements set forth above are advertisements within the meaning of N.J. Stat. Ann. § 56:8-1(a).

140. Northwell is a "person" within the meaning of N.J. Stat. Ann. § 56:8-1(d).

141. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

142. Northwell's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New Jersey Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Jersey Subclass Members' Private Information, including duties imposed by Section 5(a)(1) of the FTC Act, 15 U.S. C. § 45(a)(1),15 U.S.C. § 6801, et seq., HIPPA, 42 U.S.C. § 1301d, and COPPA, 15 U.S.C. § § 6501-05 H, and industry-standard procedures, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and New Jersey Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Jersey Subclass Members' Private Information, including duties imposed by HIPAA, COPPA, the FTC, and industry-standard procedures;

f. Failing to timely and adequately notify Plaintiffs and New Jersey Subclass Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and New Jersey Subclass Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Jersey Subclass Members' Private Information, including duties imposed by HIPAA, COPPA, the FTC, and industry-standard procedures.

143. Northwell's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Northwell's data security and ability to protect the confidentiality of consumers' Private Information.

144. Northwell's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and New Jersey Subclass Members, that their Private Information was not exposed and misled Plaintiffs and New Jersey Subclass Members into believing they did not need to take actions to secure their identities.

145. Northwell intended to mislead Plaintiffs and New Jersey Subclass Members and induce them to rely on their misrepresentations and omissions.

146. Northwell acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and New Jersey Subclass Members' rights.

147. As a direct and proximate result of Northwell's unconscionable and deceptive practices, Plaintiffs and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; the expense of purchasing multi-year identify theft protection; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

148. Plaintiffs and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

COUNT X
Violation of the New Jersey Customer Security Breach Disclosure Act,
(N.J. Stat. Ann. §§ 56:8-163 *et seq*.)
(On Behalf of the New Jersey Subclass Against All Defendants)

149. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

150. Defendants are businesses that conduct business in New Jersey, including by providing healthcare and transcription and/or dictation services at the Northwell facility in Edgewater, New Jersey.

151. Northwell "compiles or maintains computerized records that include personal information" of New Jersey residents under N.J. Stat. Ann. § 56:8-163(a).

152. PJ&A "compiles or maintains computerized records that include personal information" on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

153. Plaintiffs' and New Jersey Subclass Members' Private Information includes "personal information" covered under N.J. Stat. Ann. §§ 56:8-163, et seq.

154. Under N.J. Stat. Ann. § 56:8-163(a), "[a]ny business . . . that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay . . ."

155. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a."

156. Because Defendants discovered a breach of their security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, et seq.

157. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.J. Stat. Ann. § 56:8-163(b).

158. As a direct and proximate result of Defendants' violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiffs and New Jersey Subclass Members suffered the damages described above.

159. Plaintiffs and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class and Subclass, appointing Plaintiffs as class and subclass representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: December 6, 2023

Respectfully Submitted,

/s/ David Hilton Wise
David Hilton Wise, Esq.
Nevada Bar No. 11014
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro

Howard T. Longman *(pro hac vice forthcoming)*
LONGMAN LAW, P.C.
354 Eisenhower Parkway, Suite 1800
Livingston, New Jersey 07039
Tel: (973) 994-2315
Fax: (973) 994-2319
Email: hlongman@longman.law

Gary S. Graifman *(pro hac vice forthcoming)*
Melissa R. Emert *(pro hac vice forthcoming)*
KANTROWITZ GOLDHAMER
& GRAIFMAN, P.C.
16 Squadron Blvd, Suite 106,
New City, N.Y. 10956
Tel: 845-356-2570
Fax: 845-356-4335
ggraifman@kgglaw.com
memert@kgglaw.com

Counsel for Plaintiffs and Putative Class
**Pro Hac Vice* Application forthcoming